Docket No. 250822US6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Toshiharu TAKEMURA, et al. GAU:

SERIAL NO: New Application EXAMINER:

FILED: Herewith

FOR: DATA COMMUNICATION APPARATUS AND METHOD FOR MANAGING MEMORY IN THE SAME

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-104706	April 9, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Registration No. 40,073

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

S04P 0505 V500

850822456

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００３年 ４月 ９日

出 願 番 号
Application Number: 特願２００３－１０４７０６

[ST. 10/C]: [ＪＰ２００３－１０４７０６]

出 願 人
Applicant(s): ソニー株式会社

２００４年 ２月 ４日

特許庁長官
Commissioner,
Japan Patent Office 今 井 康 夫

出証番号 出証特２００４－３００５９１５

【書類名】　特許願

【整理番号】　0290783002

【提出日】　平成15年 4月 9日

【あて先】　特許庁長官殿

【国際特許分類】　G06K 19/07

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　竹村　俊治

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　森田　直

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　久保野　文夫

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　栗田　太郎

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　市川　琢也

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【選任した代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【手数料の表示】

【予納台帳番号】　048747

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報記憶媒体及び情報記憶媒体のメモリ管理方法

【特許請求の範囲】

【請求項１】

メモリ空間と、

前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義手段と、

サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義手段と、

を具備することを特徴とする情報記憶媒体。

【請求項２】

前記メモリ空間上に設けられた１以上のサービス・メモリ領域を含むエリアを定義するエリア定義手段をさらに備える、

ことを特徴とする請求項１に記載の情報記憶媒体。

【請求項３】

前記暗証コード・サービス定義手段は、エリア内にアクセスする前に暗証コード照合処理を行なう暗証コード・サービスを定義する、

ことを特徴とする請求項２に記載の情報記憶媒体。

【請求項４】

前記サービス定義手段により既に設けられているサービス・メモリ領域に対して適用する他のサービスを重複して定義するオーバーラップ・サービス定義手段をさらに備える、

ことを特徴とする請求項１に記載の情報記憶媒体。

【請求項５】

前記暗証コード・サービス定義手段は、前記重複して定義された他のサービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する、

ことを特徴とする請求項４に記載の情報記憶媒体。

【請求項６】

前記暗証コード・サービスによる暗証コード照合処理を有効又は無効に設定す

る照合処理制御手段をさらに含む、

ことを特徴とする請求項１に記載の情報記憶媒体。

【請求項７】

メモリ空間を備えた情報記憶媒体におけるメモリ管理方法であって、

前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義ステップと、

サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義ステップと、

を具備することを特徴とする情報記憶媒体のメモリ管理方法。

【請求項８】

前記メモリ空間上に設けられた１以上のサービス・メモリ領域を含むエリアを定義するエリア定義ステップをさらに備える、

ことを特徴とする請求項７に記載の情報記憶媒体のメモリ管理方法。

【請求項９】

前記暗証コード・サービス定義ステップでは、エリア内にアクセスする前に暗証コード照合処理を行なう暗証コード・サービスを定義する、

ことを特徴とする請求項８に記載の情報記憶媒体のメモリ管理方法。

【請求項１０】

前記サービス定義ステップにより既に設けられているサービス・メモリ領域に対して適用する他のサービスを重複して定義するオーバーラップ・サービス定義ステップをさらに備える、

ことを特徴とする請求項７に記載の情報記憶媒体のメモリ管理方法。

【請求項１１】

前記暗証コード・サービス定義ステップでは、前記重複して定義された他のサービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する、

ことを特徴とする請求項１０に記載の情報記憶媒体のメモリ管理方法。

【請求項１２】

前記暗証コード・サービスによる暗証コード照合処理を有効又は無効に設定す

る照合処理制御ステップをさらに含む、
ことを特徴とする請求項７に記載の情報記憶媒体のメモリ管理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、比較的大容量のメモリ領域を備えた情報記憶媒体及び情報記憶媒体のメモリ管理方法に係り、特に、メモリ領域上に１以上のアプリケーションが割り当てられた情報記憶媒体及び情報記憶媒体のメモリ管理方法に関する。

【０００２】

さらに詳しくは、本発明は、メモリ領域上に割り当てられているアプリケーション毎にアクセスを管理・制限する情報記憶媒体及び情報記憶媒体のメモリ管理方法に係り、特に、アプリケーションに割り当てられている個々のサービス・メモリ領域に対して複数のアクセス方法を提供する情報記憶媒体及び情報記憶媒体のメモリ管理方法に関する。

【０００３】

【従来の技術】

局所でのみ適用可能な無線通信手段の一例として、非接触ＩＣカードを挙げることができる。

【０００４】

この種の無線通信には、一般に、電磁誘導の原理に基づいて実現される。すなわち、メモリ機能を有するＩＣカードと、ＩＣカードのメモリに対して読み書きアクセスをするカード・リーダ／ライタで構成され、１次コイルとしてのＩＣカード側のループ・コイルと２次コイルとしてのカード・リーダ／ライタ側のアンテナが系として１個のトランスを形成している。そして、カード・リーダ／ライタ側からＩＣカードに対して、電力と情報を同じく電磁誘導作用により伝送し、ＩＣカード側では供給された電力によって駆動してカード・リーダ／ライタ側からの質問信号に対して応答することができる。

【０００５】

カード・リーダ／ライタ側では、アンテナに流す電流を変調することで、ＩＣ

カード上のループ･コイルの誘起電圧が変調を受けるという作用により、カード・リーダ／ライタからＩＣカードへのデータ送信を行なうことができる。また、ＩＣカードは、ループ･コイルの端子間の負荷変動により、ＩＣカード・リーダ／ライタ側のアンテナ端子間のインピーダンスが変化してアンテナの通過電流や電圧が変動するという作用により、カード・リーダ／ライタへの返信を行なう。

【０００６】

ＩＣカードに代表される非接触・近接通信システムは、操作上の手軽さから、広範に普及している。例えば、暗証コードやその他の個人認証情報、電子チケットなどの価値情報などをＩＣカードに格納しておくことにより、キャッシュ･ディスペンサやコンサート会場の出入口、駅の改札口などに設置されたカード･リーダ／ライタは、利用者がかざしたＩＣカードに非接触でアクセスして、認証処理を行なうことができる。

【０００７】

最近では、微細化技術の向上とも相俟って、比較的大容量のメモリ空間を持つＩＣカードが出現している。大容量メモリ付きのＩＣカードによれば、複数のアプリケーションを同時に格納しておくことができるので、１枚のＩＣカードを複数の用途に利用することができる。例えば、１枚のＩＣカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、多数のアプリケーションを格納しておくことにより、１枚のＩＣカードをさまざまな用途に適用させることができる。ここで言う電子マネーや電子チケットは、利用者が提供する資金に応じて発行される電子データを通じて決済（電子決済）される仕組み、又はこのような電子データ自体を指す。

【０００８】

さらに、ＩＣカードやカード用リーダ／ライタ（カード読み書き装置）が無線・非接触インターフェースの他に、外部機器と接続するための有線インターフェース（図示しない）を備えることにより、ＩＣカードやリーダ／ライタ機能を携帯電話機、ＰＤＡ（Personal Digital Assistant）やパーソナル・コンピュータなどの各デバイスにＩＣカード及びカード・リーダ／ライタのいずれか一方又は双方の機能を装備することができる。

【０００９】

このような場合、ＩＣカード技術を汎用性のある双方向の近接通信インターフェースとして利用することができる。例えば、コンピュータや情報家電機器のような機器同士で近接通信システムが構成される場合には、通信は一対一で行なわれる。また、ある機器が非接触ＩＣカードのような機器以外の相手デバイスと通信することも可能であり、この場合においては、１つの機器と複数のカードにおける一対多の通信を行なうアプリケーションも考えられる。

【００１０】

また、電子決済を始めとする外部との電子的な価値情報のやり取りなど、ＩＣカードを利用したさまざまなアプリケーションを、情報処理端末上で実行することができる。例えば、情報処理端末上のキーボードやディスプレイなどのユーザ・インターフェースを用いてＩＣカードに対するユーザ・インタラクションを情報処理端末上で行なうことができる。また、ＩＣカードが携帯電話機と接続されていることにより、ＩＣカード内に記憶された内容を電話網経由でやり取りすることもできる。さらに、携帯電話機からインターネット接続して利用代金をＩＣカードで支払うことができる。

【００１１】

ＩＣカードの一般的な使用方法は、利用者がＩＣカードをカード・リーダ／ライタをかざすことによって行なわれる。カード・リーダ／ライタ側では常にＩＣカードをポーリングしており外部のＩＣカードを発見することにより、両者間の通信動作が開始する。

【００１２】

このとき、利用者が暗証番号をＩＣカード･リーダ側に入力して、入力された暗証番号をＩＣカード上に格納された暗証番号と照合することで、ＩＣカードとＩＣカード･リーダ／ライタ間で本人確認又は認証処理が行なわれる。（ＩＣカード・アクセス時に使用する暗証番号のことを、特にＰＩＮ（Personal Identification Number）と呼ぶ。）そして、本人確認又は認証処理に成功した場合には、例えば、ＩＣカード内に保存されているアプリケーションの利用、すなわち、アプリケーションに割り当てられているサービス・メモリ領域へのアクセスが可

能となる（本明細書中では、アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ）。サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

【００１３】

本明細書中では、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

【００１４】

上述したように単一のＩＣカードが複数のアプリケーションに利用されている場合、アプリケーション毎にアクセス権を制御する必要があることから、アプリケーション毎に暗証コードを割り当てて、アプリケーション単位で照合処理してアクセスを制御することが一般的である。

【００１５】

他方、アプリケーションに対して適用することができるサービスの種類は、個々のアプリケーションが持つ性質や必要とされるセキュリティ・レベルなどの属性情報に応じて区々であるが、これ以外にも、アプリケーションの利用者毎に割り当てられているアクセス権限に応じてサービス内容を制御したいという要請がある。例えば、ユーザＡにはサービス・メモリ領域へのフルアクセスを許容してもよいが、他のユーザＢには読み出し動作しか認められない場合など、ユーザ間で差別化を図りたいである。

【００１６】

ところが、単にアプリケーションに暗証コードを割り当ててアクセスを制御するという方法では、暗証コードによって一旦照合処理を通過してしまうと、誰もがアプリケーションが定義しているサービスを一様に利用可能となる。言い換えれば、ユーザ毎にアプリケーション利用の権限を変えて、差別化を図るような場合（ユーザによって、サービス・メモリ領域への読み出し／書き込みを含んだサービスの利用を許容したり、読み出しのみのサービスの利用のみとしたりする）

であっても、すべてのユーザに対して一様なサービスを提供してしまうことになる。

【００１７】

【発明が解決しようとする課題】

本発明の目的は、メモリ領域上に１以上のアプリケーションが割り当てられた情報記憶媒体において、アプリケーションに割り当てられている個々のサービス・メモリ領域に対して、ユーザ毎に異なるアクセス権限を与え、複数のアクセス方法を提供することができる、優れた情報記憶媒体及び情報記憶媒体のメモリ管理方法を提供することにある。

【００１８】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、

メモリ空間と、

前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義手段と、

サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義手段と、

を具備することを特徴とする情報記憶媒体である。

【００１９】

また、本発明の第２の側面は、メモリ空間を備えた情報記憶媒体におけるメモリ管理方法であって、

前記メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義するサービス定義ステップと、

サービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義する暗証コード・サービス定義ステップと、

を具備することを特徴とする情報記憶媒体のメモリ管理方法である。

【００２０】

ここで言う情報記憶媒体とは、例えば、電磁誘導の原理に基づく非接触・無線通信インターフェースを備えたＩＣカードなどであり、ＩＣカード内には比較的

大容量のメモリが内蔵されている。

【００２１】

本発明によれば、メモリ空間内に、サービスを適用するサービス・メモリ領域及びサービスを定義し、さらにサービスを実行する前に暗証コード照合処理を行なう暗証コード・サービスを定義することにより、ＩＣカードのセキュアな利用を確保することができる。

【００２２】

メモリ空間上に設けられた１以上のサービス・メモリ領域を含むエリアを定義することができる。また、エリア内にアクセスする前に暗証コード照合処理を行なう暗証コード・サービスを定義するようにしてもよい。

【００２３】

サービス・メモリ領域毎に暗証コードを設定できる以外に、各エリアに対しても暗証コードを設定することができるので、メモリ領域へのアクセス権を階層的に制御することができる。また、複数のサービスに対して共通の暗証コードを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。

【００２４】

例えば、あるエリアに該当する暗証コードを入力することにより、照合・認証処理を経て、エリア内のすべてのサービス・メモリ領域（並びにサブエリア）へのアクセス権を与えるようにすることもできる。したがって、例えば、該当するエリアに対する暗証コードの入力を１回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。

【００２５】

また、既に設けられているサービス・メモリ領域に対して適用する他のサービスを重複して定義する、すなわちオーバーラップ・サービスを定義するようにしてもよい。

【００２６】

オーバーラップ・サービスを定義することにより、あるサービス・メモリ領域

に対して、「読み出しのみ」、「読み出し及び書き込み」など複数のアクセス方法を設定することができる。

【００２７】

また、オーバーラップ・サービス定義を行なう場合、サービス毎に暗証コードを設定するようにしてもよい。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々の暗証コードが設定される。また、あるメモリ領域に対する読み出しについては暗証コードの入力が必要でないが、書き込む場合には暗証コードの入力を必須とさせることが可能である。

【００２８】

また、暗証コード・サービスによる暗証コード照合処理を有効又は無効に設定する照合処理の制御を行なうようにしてもよい。

【００２９】

サービス又はエリアに対する暗証コード・サービスが有効になっている場合にのみ、サービスの起動又はエリアへのアクセスを行なう前に暗証コードの照合が要求され、暗証コード・サービスが無効にされている場合には暗証コードの照合は要求されない。

【００３０】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３１】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態について詳解する。

【００３２】

<u>Ａ．非接触通信システム</u>

本発明は、ＩＣカードを利用した非接触データ通信システムに関するものである。この種の非接触データ通信システムは、一般に、電磁誘導の原理に基づいて実現される。すなわち、メモリ機能を有するＩＣカードと、ＩＣカードのメモリ

に対して読み書きアクセスをするカード・リーダ／ライタで構成され、１次コイルとしてのＩＣカード側のループ・コイルと２次コイルとしてのカード・リーダ／ライタ側のアンテナが系として１個のトランスを形成している。カード・リーダ／ライタ側からＩＣカードに対して、電力と情報を同じく電磁誘導作用により質問信号を伝送する。そして、ＩＣカード側では供給された電力によって駆動し、質問信号に対する応答信号に応じて自身のアンテナ間の負荷を変化させることによって読み書き装置の受信回路に現れる信号に振幅変調をかけて通信を行なう。なお、以下の説明では、携帯端末などに内蔵して使用されるＩＣチップも含めて、「ＩＣカード」と呼ぶことにする。

【００３３】

図１には、電磁誘導に基づくリーダ／ライタ１０１とＩＣカード５０との無線通信の仕組みを概念的に図解している。リーダ／ライタ１０１は、ループ･コイルで構成されたアンテナL_{RW}を備え、このアンテナL_{RW}に電流I_{RW}を流すことでその周辺に磁界を発生させる。一方、ＩＣカード５０側では、電気的にはＩＣカード５０の周辺にループ･コイルL_cが形設されている。ＩＣカード５０側のループ･コイルＬc端にはリーダ／ライタ１０１側のループ・アンテナL_cが発する磁界による誘導電圧が生じ、ループ･コイルＬc端に接続されたＩＣカード５０の端子に入力される。

【００３４】

リーダ／ライタ１０１側のアンテナL_{RW}とＩＣカード５０側のループ･コイルL_cは、その結合度は互いの位置関係によって変わるが、系としては１個のトランスを形成していると捉えることができ、図２に示すようにモデル化することができる。

【００３５】

リーダ／ライタ１０１は、アンテナL_{RW}に流す電流I_{RW}を変調することで、ＩＣカード上のループ･コイルL_cに誘起される電圧V_0は変調を受け、そのことを利用してリーダ／ライタ１０１はＩＣカード５０へのデータ送信を行なうことができる。ここで言う送信データには、リーダ／ライタ１０１に接続された外部機器側でユーザ入力された暗証番号やパスワードなどの、アプリケーションやエリ

アへのアクセス権を得るための暗証コードや、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【００３６】

また、ＩＣカード５０は、リーダ／ライタ１０１へ返送するためのデータに応じてループ･コイルL_Cの端子間の負荷を変動させる機能（Load Switching）を持つ。ループ･コイルL_Cの端子間の負荷が変動すると、リーダ／ライタ１０１側ではアンテナ端子間のインピーダンスが変化して、アンテナL_{RW}の通過電流I_{RW}や電圧V_{RW}の変動となって現れる。この変動分を復調することで、リーダ／ライタ１０１はＩＣカード５０の返送データを受信することができる。リーダ／ライタ１０１がＩＣカード５０から受信するデータには、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【００３７】

Ｂ．ＩＣカード内のメモリ空間の構造

携帯端末１０に内蔵されたＩＣカード５０内のメモリには、電子決済を始めとする外部との電子的な価値情報のやり取りなど、１以上のアプリケーションが割り当てられている。アプリケーションに割り当てられているメモリ領域を「サービス・メモリ領域」と呼ぶ。また、アプリケーションの利用、すなわち該当するサービス・メモリ領域へアクセスする処理動作のことを「サービス」と呼ぶ。サービスには、メモリへの読み出しアクセス、書き込みアクセス、あるいは電子マネーなどの価値情報に対する価値の加算や減算などが挙げられる。

【００３８】

ユーザがアクセス権を持つかどうかに応じてアプリケーションの利用すなわちサービスの起動を制限するために、アプリケーションに対して暗証コードを割り当て、サービス実行時に暗証コードの照合処理を行なうようになっている。また、サービス・メモリ領域へのアクセスは、アプリケーションのセキュリティ・レベルなどに応じて、適宜暗号化通信が行なわれる。

【００３９】

本実施形態では、ＩＣカード５０内のメモリ空間に対して、「ディレクトリ」に類似する階層構造を導入する。そして、メモリ領域に割り当てられた各アプリ

ケーションを、所望の階層の「エリア」に登録することができる。例えば、一連のトランザクションに使用される複数のアプリケーション、あるいは関連性の深いアプリケーション同士を同じエリア内のサービス・メモリ領域登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことによって、メモリ領域のアプリケーションやエリアの配置が整然とし、ユーザにとってはアプリケーションの分類･整理が効率化する。

【００４０】

また、メモリ領域へのアクセス権を階層的に制御するために、アプリケーション毎に暗証コードを設定できる以外に、各エリアに対しても暗証コードを設定することができるようにした。例えば、あるエリアに該当する暗証コードを入力することにより、照合・認証処理を経て、エリア内のすべてのアプリケーション（並びにサブエリア）へのアクセス権を与えるようにすることもできる。したがって、例えば、該当するエリアに対する暗証コードの入力を１回行なうだけで、一連のトランザクションで使用されるすべてのアプリケーションのアクセス権を得ることができるので、アクセス制御が効率化するとともに、機器の使い勝手が向上する。

【００４１】

さらに、本実施形態において特徴的なのは、あるサービス・メモリ領域に対するアクセス権限が単一でないことを許容し、それぞれのアクセス権限毎、すなわちサービス・メモリ領域において実行するサービスの内容毎に、暗証コードを設定することができるという点である。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定される。また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々の暗証コードが設定される。また、あるメモリ領域に対する読み出しについては暗証コードの入力が必要でないが、書き込む場合には暗証コードの入力を必須とさせることが可能である。適用するサービス毎に暗証コードを設定する点については、後に詳解する。

【００４２】

図３には、本実施形態に係るＩＣカード５０内の機能構成を図解している。同

図に示すように、ＩＣカード５０は、リーダ／ライタ１０１と無線通信を行なうアンテナが接続されるＲＦ部５１と、アプリケーション毎に割り当てられたサービス・メモリ領域を持つメモリ５２（前述）と、ＲＦ部５１などから入力された暗証コードの比較照合を行なう照合部５３と、これらの構成部品を統括的にコントロールする制御部５５とからなる。

【００４３】

制御部５５は、ＣＰＵ（Central Processing Unit），ＲＯＭ（Read Only Memory），ＲＡＭ（Random Access Memory）などを一体化して構成されている。制御部５５は、ＲＯＭに格納されたプログラム･コードを実行することによって、ＩＣカード５０内の動作を制御する。

【００４４】

メモリ５２は、１以上のアプリケーションに対して記憶領域を割り当てるために使用される。メモリ５２は、半導体メモリの他、磁気ストライプなど、読み書き可能な記憶媒体であればよく、特定のデバイスには限定されない。

【００４５】

本実施形態では、メモリ５２が持つ記憶空間には、「ディレクトリ」に類似する階層構造が導入されている。すなわち、メモリ領域に割り当てられた各アプリケーションを、所望の階層エリアにサービス・メモリ領域として登録することができる。例えば、一連のトランザクションに使用されるアプリケーションなど、関連性の深いアプリケーション同士を同じエリアに登録する（さらには、関連性の深いエリア同士を同じ親エリアに登録する）ことができる。

【００４６】

また、メモリ５２内に割り当てられたアプリケーション（すなわちサービス・メモリ領域）並びにエリアは暗証コード定義ブロックを備えている。したがって、アプリケーション毎に、あるいはエリア毎に暗証コードを設定することができる。また、メモリ５２に対するアクセス権は、アプリケーション単位で行なうとともに、並びにエリア単位で行なうことができる。

【００４７】

さらに、あるサービス・メモリ領域に対するアクセス権限が単一でなく、実行

するサービスの内容毎に、暗証コードを設定することができる。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定され、また、電子マネーやその他の価値情報に対する「増額」と「減額」とでは、別々の暗証コードが設定される（後述）。

【００４８】

照合部５３は、例えばＲＦ部５１を介して送られてくる暗証コードを、各アプリケーション又はディレクトリに割り当てられたエリア又はサービス・メモリ領域に設定されている暗証コードと照合して、一致するメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、ＲＦ部５１を介してリーダ／ライタ１０１から読み書きが可能となる。

【００４９】

Ｃ．暗証コードの適用

上述したようにＩＣカード内のメモリには、アプリケーションに割り当てられたさまざまなサービス・メモリ領域が割り当てられており、各サービス・メモリ領域に対して適用可能な１以上のサービスが設けられている。本実施形態では、エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、アプリケーションに適用されるサービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。

【００５０】

図４には、ＩＣカード５０のメモリ空間の基本構成を示している。図３を参照しながら既に説明したように、ＩＣカード５０内のメモリ空間に対して、「ディレクトリ」に類似する階層構造が導入され、所望の階層のエリアに、アプリケーションに割り当てられたサービス・メモリ領域を登録することができる。同図に示す例では、エリア０００００定義ブロックで定義されるエリア０００００内に、１つのサービス・メモリ領域が登録されている。

【００５１】

図示のサービス・メモリ領域は、１以上のユーザ・ブロックで構成される。ユーザ・ブロックはアクセス動作が保証されているデータ最小単位のことである。

このサービス・メモリ領域に対しては、サービス０１０８定義ブロックで定義されている１つのサービスすなわちサービス０１０８が適用可能である。

【００５２】

本実施形態では、エリア単位、並びにアプリケーション単位でアクセス制限を行なう以外に、サービスの種類毎に暗証コードを設定して、サービス単位でアクセス制限を行なうことができる。アクセス制限の対象となるサービスに関する暗証コード設定情報は、暗証コード専用のサービス（すなわち「暗証コード・サービス」）として定義される。

【００５３】

図４に示す例では、サービス０１０８に関する暗証コードが暗証コード・サービス０１２８定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

【００５４】

サービス０１０８に対する暗証コード・サービスが有効になっている場合、サービス０１０８を起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なう前に、暗証コード・サービス０１２８を使用した暗証コードの照合が必要となる。具体的には、暗号化あり読み書き（Read/Write）コマンドを使用する場合は、相互認証前にサービス０１０８に対する暗証コードの照合を行なう。（暗証コード・サービスを有効／無効にする仕組みについては後述に譲る。）

【００５５】

また、本実施形態では、アプリケーションに割り当てられたサービス・メモリ領域を所望の階層のエリアに登録するとともに、エリアを階層化する（関連性の深いエリア同士を同じ親エリアに登録する）ことができる。この場合、エリア毎に暗証コードを設定することにより、エリアをアクセス制限の単位とすることができる。

【００５６】

図５には、ＩＣカード５０のメモリ空間においてエリアが階層化されている様子を示している。同図に示す例では、エリア０００００定義ブロックで定義されているエリア０００００内に、エリア１０００定義ブロックで定義されている別のエ

リア１０００が登録されている。

【００５７】

図５に示す例では、さらにエリア１０００内には、２つのサービス・メモリ領域が登録されている。一方のサービス・メモリ領域に対しては、サービス１１０８定義ブロックで定義されているサービス１１０８と、サービス１１０Ｂ定義ブロックで定義されているサービス１１０Ｂが適用可能である。このように、１つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義することを、本明細書中では「オーバーラップ・サービス」と呼ぶ。オーバーラップ・サービスにおいては、同じサービス・エリアに対して、入力した暗証コードに応じて異なるサービスが適用されることになる。

【００５８】

また、他方のサービス・メモリ領域に対しては、サービス１１０Ｃ定義ブロックで定義されているサービス１１０Ｃが適用可能である。

【００５９】

各サービス・メモリ領域に設定されているサービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことができる。勿論、図４を参照しながら説明したように、サービス毎に暗証コード・サービスを定義することができる。この場合、サービスに対する暗証コード・サービスが有効になっているときには、暗証コード・サービスを使用した暗証コードの照合を行なってからサービスの起動が許可される。

【００６０】

また、複数のサービスに対して共通の暗証コードを設定したい場合には、これらサービスを含むエリアを作成し、このエリアに対して共通の暗証コード・サービスを適用することができる。

【００６１】

図５に示す例では、エリア１０００に関する暗証コードが、暗証コード・サービス１０２０定義ブロックとして定義されている。その暗証コード・サービスの内容は暗証コード・サービス・データ・ブロックに格納されている。

【００６２】

エリア１０００に対する暗証コード・サービスが有効（後述）になっている場合、暗証コード・サービス１０２０を使用した暗証コードの照合を行なった後に、エリア１０００内の各サービスを起動してそのユーザ・ブロックに読み出し又は書き込み動作を行なうことが可能となる。

【００６３】

ここで、エリア１０００内のサービスに暗証コード・サービスが適用されており且つこれが有効となっている場合には、さらにその暗証コード・サービスを使用した暗証コードの照合を経てからでないと、そのユーザ・ブロックに読み出し又は書き込み動作を行なうことはできない。

【００６４】

図４及び図５に例示したように、暗証コード照合の対象となるエリアやサービスに対応する暗証コード・サービスは一意に与えられる。

【００６５】

D．暗証コード・サービスの登録

暗証コード・サービスのＩＣカード５０への登録は、通常のサービスと同様の登録サービス・コマンドを使用して行なう。

【００６６】

但し、暗証コード・サービスの登録は、暗証コード照合の対象となるエリアやサービスが既にＩＣカード５０に登録済みであることが条件となる。すなわち、暗証コード照合の対象となるエリアやサービスがない場合は、暗証コード・サービスの登録サービス実行時にエラーとなる。

【００６７】

また、暗証コード・サービスは、通常のサービスのユーザ・ブロックに相当する暗証コード・サービス・データ・ブロックが１ブロックしか存在しないので、サービス登録時に登録サービス・コマンドで指定ユーザ・ブロック数を１以外の値に設定するとエラーとなる。

【００６８】

図６には、ＩＣカード５０内のメモリ空間にエリアやサービスを登録するための手順を示している。

【００６９】

まず、メモリ空間にエリアが定義される（ステップＳ１）。

【００７０】

次いで、サービスの登録サービス・コマンドを使用して、エリア内にアプリケーションに対してサービス・メモリ領域を割り当てるとともに、このサービス・メモリ領域に適用されるサービスを定義する（ステップＳ２）。登録サービス・コマンドでは、サービス・メモリ領域のユーザ・ブロック数を指定する。エリア内で複数のアプリケーションを割り当てたい場合には、当該処理ステップを繰り返し実行する。

【００７１】

エリア内で定義したサービスに対して暗証コードを適用したい場合には、サービスの登録サービス・コマンドを使用して、暗証コード・サービスの登録を行なう（ステップＳ３）。

【００７２】

さらに、エリア内で定義されたすべてのサービスに対して共通の暗証コードを設定したい場合には、サービスの登録サービス・コマンドを使用して、このエリアに対して共通の暗証コード・サービスの登録を行なう（ステップＳ４）。

【００７３】

なお、ステップＳ３とステップＳ４の実行順序は逆であってもよい。

【００７４】

さらに、１つのサービス・メモリ領域に対してサービス内容の異なる複数のサービスを定義したい場合には、サービスの登録サービス・コマンドを使用して、オーバーラップ・サービス（図５を参照のこと）を登録する（ステップＳ５）。

【００７５】

そして、オーバーラップ・サービスに対して暗証コードを適用したい場合には、サービスの登録サービス・コマンドを使用して、暗証コード・サービスの登録を行なう（ステップＳ６）。

【００７６】

図４に示した例では、ルートのエリア００００内にサービス・メモリ領域の割

り当て並びにこれに適用するサービス０１０８が登録された後、サービス０１０８に適用される暗証コード・サービスが登録される。

【００７７】

また、図５に示した例では、ルートのエリア００００下のエリア１０００内で、２つのサービス・メモリ領域が割り当てられるとともに、それぞれに適用されるサービス１１０８、サービス１１０Ｃが登録される。また、一方のサービス・メモリには、他のサービス１１０Ｂがオーバーラップ・サービスとして登録される。図示しないが、これらに暗証コードを適用したい場合には、別途、暗証コード・サービスの登録が行なわれる。そして、登録されたサービス１１０８，１１０Ｂ，１１０Ｃに対して共通の暗証コードを設定したい場合には、エリア１０００に対して共通の暗証コード・サービスを登録する。

【００７８】

Ｅ．暗証コードの適用

図４及び図５に例示したように、ＩＣカード５０内のメモリ空間に登録されたエリアやサービスに対して暗証コードを適用して、エリア単位、あるいはサービス単位でアクセス制御を行なうことができる。また、１つのサービス・メモリ領域に対して複数のサービス（オーバーラップ・サービス）を登録することができるが、サービス毎に暗証コードを適用することで、同じサービス・メモリ領域に対して複数のアクセス方法を定義することができる。

【００７９】

暗証コードの適用内容は、暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックに記述されている。図７には、暗証コード・サービス・データ・ブロックのデータ構造を模式的に示している。同図に示すように、暗証コード定義領域は、暗証番号領域と、入力失敗回数記憶領域と、最大許容入力失敗回数設定領域と、暗証番号使用選択領域と、アクセス許可フラグとで構成されている。

【００８０】

ユーザが入力した暗証コードが一致した場合にのみ、該当するサービス又はエリアの暗証コード・サービス・データ・ブロック内のアクセス許可フラグを立て

て、其処へのアクセスを許可する。

【００８１】

アクセス許可フラグは、該当するアプリケーション又はディレクトリのアクセス可否状態を示すためのフラグであり、アクセス許可フラグが設定されたサービス又はエリアはアクセス許可状態である。暗証コードが設定されたサービスやエリアのアクセス許可フラグは、デフォルトではアクセス不可状態であり、暗証コードの照合処理や秘密鍵を用いた認証処理に成功した後、アクセス許可フラグが設定されて、アクセス許可状態に転じる。また、アクセス許可フラグを設定し続けると、ＩＣカード５０又は携帯端末１０が紛失した場合や盗難に遭った場合にサービスやエリアの無断使用･不正使用によりユーザが損害を被るおそれがある。このため、ＩＣカード５０は、例えばＲＦ部５１において電磁波が途絶えたことに応答してアクセス許可状態を自動的にアクセス不可にする機構を備えていてもよい。

【００８２】

また、誤った暗証コードが入力された場合には、その都度、入力失敗回数記憶領域の記録を更新する。そして、入力失敗回数が最大許容入力失敗回数設定領域に設定された最大許容入力失敗回数に到達した場合には、該当するサービスの起動又はエリアに対するアクセスを禁止する。

【００８３】

一般には、この入力失敗回数は、一度入力に成功したらクリアするべきものである。このようにして悪意あるユーザがしらみつぶしに暗証コードを調べることを防止する。また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、ＩＣカード５０を管理する管理者のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば後述するような秘密鍵による認証を使用することもできる。

【００８４】

図８には、ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順をフローチャートの形式で示している。

【００８５】

ユーザから暗証コードを入力すると（ステップＳ１１）、照合部５３は、各暗証コード・サービス定義ブロックの暗証コード・サービス・データ・ブロックにアクセスして、暗証コードが一致するか否かを判別する（ステップＳ１２）。

【００８６】

暗証コード・サービス・データ・ブロックの暗証コードがユーザ入力された暗証コードと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、対応するサービス又はエリアをアクセス可能状態にする（ステップＳ１３）。

【００８７】

暗証コードは、例えば、ＩＣチップ５０をリーダ／ライタ１０１にかざして、リーダ／ライタ１０１に接続されている外部機器（図示しない）のユーザ･インターフェースを用いて入力したものを、無線インターフェースすなわちＲＦ部５１経由でＩＣチップに送信することができる。

【００８８】

図８に示すように暗証コードを用いてアプリケーションやディレクトリへのアクセス権を制御する場合、悪意のあるユーザはしらみつぶしに暗証コードを調べることにより、セキュリティの壁が破られる可能性がある（特に桁数の少ない暗証コードを用いる場合）。このため、本実施形態では、暗証コード定義領域において、最大許容入力回数を設定して、入力失敗回数が最大許容入力回数に到達したアプリケーション又はディレクトリをアクセス不可状態に設定することで、アクセス制御を行なうようにしている。

【００８９】

図９には、暗証コードの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順をフローチャートの形式で示している。

【００９０】

ユーザから暗証コードを入力すると（ステップＳ２１）、照合部５３は、各暗証コード・サービス定義ブロックにアクセスして、暗証コードが一致するか否かを判別する（ステップＳ２２）。

【００９１】

ユーザ入力された暗証コードが暗証コード・サービス定義ブロックの暗証コードと一致する場合には、その暗証コード・サービス・データ・ブロック内のアクセス許可フラグを設定して、該当するサービス又はエリアをアクセス可能状態にする（ステップＳ２３）。

【００９２】

他方、ユーザ入力された暗証コードがいずれの暗証コード・サービス定義ブロックの暗証コードとも一致しない場合には、暗証コード定義領域内の入力失敗回数を更新する（ステップＳ２４）。また、ユーザ入力された暗証コードがいずれの暗証コード・サービス定義ブロックの暗証コードと一致し、照合に成功した場合には、入力失敗回数を０にクリアする。

【００９３】

そして、ステップＳ２５では、更新された入力失敗回数が、暗証コード定義領域内で設定されている最大許容入力回数に到達したか否かを判断する（ステップＳ２５）。

【００９４】

もし、入力失敗回数が最大許容入力回数に到達してしまったならば、その暗証コード定義領域内のアクセス許可フラグの設定を解除して、該当するサービス又はエリアをアクセス不可状態にする（ステップＳ２６）。この結果、悪意のあるユーザがしらみつぶしに暗証コードを調べる行為を取り締まることができる。

【００９５】

また、ユーザが誤って最大許容入力失敗回数に達して暗証コード入力に失敗してしまった場合は、ＩＣカード５０を管理する管理者のみが入力失敗回数記憶領域をクリアできるようにしてもよい。この管理者の認証には、例えば秘密鍵による認証を使用することもできる。

【００９６】

Ｆ．暗証コード比較出力の制御

既に述べたように、サービス又はエリアに対する暗証コード・サービスが有効になっている場合にのみ、サービスの起動又はエリアへのアクセスを行なう前に

、暗証コードの照合が要求され、暗証コード・サービスが無効にされている場合には、暗証コードの照合は要求されない。

【００９７】

この項では、暗証コード・サービスの有効／無効の設定による暗証コード比較出力の制御について説明する。

【００９８】

図１０には、ＩＣカード５０における暗証コード比較出力の制御に関する機能構成を模式的に示している。

【００９９】

同図に示すように、ＩＣカード５０は、非接触・無線インターフェースなどからなる通信部１５１と、価値情報などのデータを保持するデータ保持部１５２と、データ保持部１５２へのアクセスを制御する暗証コードを保持する暗証コード保持部１５３と、通信部１５１から入力された暗証コードと暗証コード保持部１５３に保持されている暗証コードとを比較照合する暗証コード比較部１５４と、暗証コード比較を行なう条件に従って暗証コード比較出力を制御するフロー制御部１５５とを備えており、暗証コード識別装置を構成する。

【０１００】

通信部１５１では、図１１に示すように、１バイト単位にデータが送受信されるものとする。同図において、１バイト・データの開始は、必ずスタート・ビットで開始するものとする。その後、８ビット分のデータが続き、最後にストップ・ビットが来る。各ビット長は、固定で、送受信者間で事前に取り決めておくものとする。

【０１０１】

また、図１２には、１バイト・データが集まって構成されるパケットの構成を模式的に示している。同図に示すように、パケットの前半はコード部であり、また、パケットの後半はデータ部（ペイロード）となっている。コード部には、そのパケットの意味付けを示すデータが記述されている。また、データ部は、コードに付随する何らかのデータ（データ本体）が必要な場合に添付されている。

【０１０２】

また、図１３には、送受信者間におけるパケット交換の基本シーケンスを示している。本実施形態においては、送信者を外部装置１００とし、受信者を暗証コード識別装置としてのＩＣカード５０とする。

【０１０３】

パケットは、送信者から受信者へ何らかのアクションを要求するコマンドと、そのコマンドのアクションの結果として、受信者から送信者へ返送されるレスポンスに分けることができる。本実施形態で使用するコマンドとレスポンスを、以下の表に示しておく。

【０１０４】

【表１】

コマンド(外部装置→識別装置)		レスポンス(識別装置→外部装置)		意味
コード部	データ部	コード部	データ部	
１０ｈ	暗証コード	１２ｈ	ＯＫ／ＮＧ	暗証コード入力
１８ｈ	暗証コード	１Ａｈ	ＯＫ／ＮＧ	暗証コード変更
２０ｈ	読み出し位置	２２ｈ	ＯＫ(読み出したデータ)／ＮＧ	データ読み出し
３０ｈ	書き込みデータ，書き込み位置	３２ｈ	ＯＫ／ＮＧ	データ書き込み
４０ｈ	フラグ値	４２ｈ	ＯＫ／ＮＧ	有効/無効 変更
５０ｈ	フラグ値	５２ｈ	ＯＫ／ＮＧ	無効→有効 変更
６０ｈ	フラグ値	５４ｈ	ＯＫ／ＮＧ	有効→無効 変更

【０１０５】

コマンドのコード部１０ｈは、データ部に設定した暗証コードを暗証コード識別装置としてのＩＣカード５０へ入力することを示す。通信部１５１によってコード部が解釈されると、引き続くデータ部が、暗証コード比較部５４へ伝達されることになる。

【０１０６】

暗証コード比較部１５４は、伝達されたデータ部と暗証コード保持部１５３内に保持されている暗証コードとを比較し、一致している場合は、一致出力を出力する。そして、フロー制御部１５５は、データ保持部１５２と通信部１５１間でのデータ伝送を制限する機能を有する。

【０１０７】

図１４には、フロー制御部１５５の構成を示している。

【０１０８】

有効／無効フラグ１５５Ａは、データ保持部１５２と通信部１５１間の伝送路を接続状態とするか非接続状態とするかを、暗証コード比較部１５４の比較出力に応じて決定するかどうかを示すフラグである。

【０１０９】

有効／無効フラグ１５５Ａが”１”で有効側のときには、スイッチ２は比較出力側となる。そして、暗証コード比較部１５４の出力が一致を出力している場合には、それがスイッチ１へ伝わってスイッチ１をオン状態とし、データ保持部１５２と通信部１５１の伝送路を接続状態とすることで、外部装置１００が通信部１５１を介してデータ保持部１５２へのアクセスが可能となる。また、暗証コード比較部１５４の出力が不一致の場合には、それがスイッチ１へ伝わってスイッチ１をオフ状態とし、データ保持部１５２と通信部１５１の伝送路を非接続とすることで、外部装置１００は通信部１５１を介してデータ保持部１５２にアクセスすることができない。

【０１１０】

他方、有効／無効フラグ１５５Ａが”０”で無効側のときには、スイッチ２は常時オン側となる。したがって、暗証コード比較部１５４の比較出力によらず、スイッチ１を常時オン状態とし、データ保持部１５２と通信部１５１の伝送路の接続状態を維持する。

【０１１１】

この有効／無効フラグ１５５Ａによって、暗証コード比較が不必要な場合には、その機能を抑制すなわち暗証コード・サービスを無効にすることが可能となるという点を充分理解されたい。

【０１１２】

無効→有効フラグ１５５Ｂは、コマンド・コード５０ｈによって変更することができるフラグである。無効→有効フラグ１５５Ｂは、後述するコマンド・コード４０ｈによって有効／無効フラグを、”０”の無効の状態から”１”の有効の

状態へ書き換えを行なう際に暗証コードの一致が必要かどうかを選択するためのフラグである。すなわち、無効→有効フラグが”１”のときには本動作が成され、有効／無効フラグ１５５Ａが”０”で暗証コード比較が無効であって且つ比較出力が一致している場合には、スイッチ３をオンの状態にして、通信部１５１からの有効／無効フラグ１５５Ａの書き換えを許可する。一方、無効→有効フラグが”０”のときには、フラグ判別部１５５Ｄの出力部の出力は常にスイッチ３をオンの状態にして、通信部１５１からの有効／無効フラグ１５５Ａの書き換えを常に許可する。

【０１１３】

無効→有効フラグ１５５Ｂが”１”の場合には、有効／無効フラグ１５５Ａを無効から有効に変更する際に暗証コードの一致が必要であることを示す。また、無効→有効フラグ１５５Ｂが”０”の場合には、有効／無効フラグ１５５Ａを無効から有効に変更する際に暗証コードの一致が不必要であることを示す。

【０１１４】

一方、有効→無効フラグ１５５Ｃは、コマンド・コード６０ｈによって変更することができるフラグである。有効→無効フラグ１５５Ｃは、後述するコマンドコード４０ｈによって有効／無効フラグ１５５Ａを、”１”の有効の状態から”０”の無効の状態へ書き換えを行なう際に、暗証コードの一致が必要かどうかを選択するためのフラグである。すなわち、有効→無効フラグ５５Ｃが”１”のときに本動作が成され、有効／無効フラグ１５５Ａが”１”で暗証コード比較が有効であって且つ比較出力が一致している場合には、スイッチ３をオンの状態にして、通信部１５１からの有効／無効フラグ１５５Ａの書き換えを許可する。一方、有効→無効フラグが”０”のときには、フラグ判別部１５５Ｄの出力部の出力は常にスイッチ３をＯＮの状態にして、通信部５１からの有効／無効フラグ１５５Ａの書き換えを常に許可する。

【０１１５】

有効→無効フラグ１５５Ｃが”１”の場合には、有効／無効フラグ１５５Ａを有効から無効に変更する際に暗証コードの一致が必要であることを示す。また、有効→無効フラグ１５５Ｃが”０”の場合には、有効／無効フラグ１５５Ａを有

効から無効に変更する際に暗証コードの一致は不必要である。

【０１１６】

上述したような有効／無効フラグの変更制御オペレーションは、フラグ判別部１５５Ｄによって行なわれる。このオペレーションを論理的に整理すると、フラグ判別部１５５Ｄの出力は、以下の［表２］に示す通りとなる。

【０１１７】

【表２】

		有効／無効			
		1		0	
		比較出力		比較出力	
		一致	不一致	一致	不一致
無効→有効	1	0	0	1	0
	0	0	0	1	1
有効→無効	1	1	0	0	0
	0	1	1	0	0

【０１１８】

コマンド・コード４０ｈは、有効／無効フラグ１５５Ａを変更するためのコマンドであり、上述した動作により、スイッチ３がオンの状態のときにのみ通信部１５１からの変更が可能である。

【０１１９】

このような仕組みにより、暗証コードを変更する際に、暗証コードを無効な状態から有効な状態にするには暗証コードを入力する必要はないが、逆に、暗証コードを有効な状態から無効な状態にするには暗証コードを入力する必要があるといったように、暗証コードの入力条件をさまざまに組み合わせて設定することが可能となる。

【０１２０】

以上説明したような処理オペレーションを経て、スイッチ１がオン状態になるとデータ保持部１５２と通信部１５１が接続状態となるため、それ以降は、リーダ／ライタ１０１側では、コマンド・コード２０ｈによってデータ保持部１５２

内の所定位置からデータの読み出しを行なったり、コマンド・コード３０ｈによって所定データをデータ保持部１５２に書き込んだりすることが可能になる。

【０１２１】

暗証コード保持部１５３に既に書き込まれている暗証コードを書き換える際には、コマンド・コード１８ｈを使用する。書き換えが可能かどうかは、スイッチ４によって制御することが可能である。

【０１２２】

図１４に示す例では、前述の無効→有効フラグ１５５Ｂ、有効→無効フラグ１５５Ｃのそれぞれの状態、有効／無効フラグ１５５Ａの状態、並びに、暗証コード比較部１５４の状態に応じて、フラグ判別部１５５Ｄによって制御するようになっている。すなわち、それぞれのフラグの状態に応じてスイッチ４の制御条件を変更することができ、例えば、無効→有効フラグ１５５Ｂが”０”から”１”にセットされる際に暗証コード保持部１５３の暗証コードを変更するようにすることも可能である。これによって、暗証コードの判別を有効にするときには、それ以前に設定されていた暗証コードに関係なく、新たな暗証コードを設定することが可能である。簡単なコマンド操作によって設定の書き換えを行なうことができるが、通信部１５１とリーダ／ライタ１０１との間に相互認証手段を挿入することで、セキュリティ・レベルを高めることも可能である。

【０１２３】

図３～図５に示したようにＩＣカード５０内のメモリ領域が拡張されて、複数のアプリケーション（サービス・メモリ領域）が割り当てられている場合など、複数の暗証コードを用いてアクセス権を制御する場合においても、図１０に示した暗証コード比較出力の仕組みを適用することができる。

【０１２４】

図１５には、暗証コード保持部及び暗証コード比較部を複数個装備した暗証コード識別装置（ＩＣカード５０）の構成例を示している。図１５に示す例では、複数の暗証コード比較部１５４においてすべてが一致出力を出力したときにのみ、データ保持部１５２と通信部１５１が接続状態になるように構成する。これによって、暗証コードを入力する一部のリーダ／ライタ１０１を個人ユーザとする

とともに、暗証コードを入力する他の一部のリーダ／ライタ１０１を運用する運用者（例えば、当該カード･サービスの管理者など）に割り当てることにより、運用者側の判断によって、暗証コード機能を制御することが可能となる。例えば、利用者の意思に拘わらず、強制的に暗証コードの入力が必要なように設定することが可能となる。

【０１２５】

また、図１６には、データ保持部１５２の個々のメモリ領域に対して暗証コードをそれぞれ設定できるようにした暗証コード識別装置（ＩＣカード５０）の構成例を示している。

【０１２６】

暗証コード比較部１５４は、データ保持部１５２に割り当てられた各メモリ領域と暗証コードとの関係を示したルックアップ･テーブルを持っており、そのルックアップ･テーブルに従って、通信部１５１から入力された暗証コードが該当するメモリ領域の暗証コードと一致しているか否かを判別することができる。そして、互いの暗証コードが一致する場合には、該当するメモリ領域のアクセスを可能にする。以下の［表３］には、暗証コード比較部１５４において管理されるルックアップ･テーブルの構成例を示している。

【０１２７】

【表３】

暗証コード	許容メモリ開始アドレス	許容メモリ終了アドレス
暗証コード１	１００ｈ	１８０ｈ
暗証コード２	３００ｈ	３Ａ０ｈ
暗証コード３		
⋮	⋮	⋮

【０１２８】

このような構成によれば、通信部１５１を介して入力された暗証コードは、各

暗証コード比較部１５４において、ルックアップ･テーブル中に保持されているそれぞれの暗証コードと比較が行なわれる。そして、データ保持部１５２が持つメモリ空間のうち一致出力が得られた暗証コードに該当するメモリ領域に対するアクセスを許可するようにすることができる。

【０１２９】

［追補］

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１３０】

【発明の効果】

以上詳記したように、本発明によれば、メモリ領域上に１以上のアプリケーションが割り当てられた情報記憶媒体において、アプリケーションに割り当てられている個々のサービス・メモリ領域に対して、ユーザ毎に異なるアクセス権限を与え、複数のアクセス方法を提供することができる、優れた情報記憶媒体及び情報記憶媒体のメモリ管理方法を提供することができる。

【０１３１】

本発明によれば、ＩＣカード上のあるメモリ領域に対するアクセス権限が単一でない場合であっても、それぞれのアクセス権限に応じて暗証コードを個別に設定することができる。すなわち、同じサービス・メモリ領域について、適用すべきサービス毎に暗証コードが設定される。例えば、あるメモリ領域に対する読み出しについては暗証コードの入力が必要でないが、書き込む場合には暗証コードの入力を必須とさせることが可能である。

【図面の簡単な説明】

【図１】

電磁誘導に基づくリーダ／ライタ１０１とＩＣカード５０との無線通信の仕組みを説明するための図である。

【図２】

リーダ／ライタ１０１とＩＣカード５０からなる系を１個のトランスとして捉えてモデル化した図である。

【図３】

ＩＣカード５０内の機能構成を示した図である。

【図４】

サービスに対して暗証コードを適用するための仕組みを説明するための図である。

【図５】

エリアに対して暗証コードを適用するための仕組みを説明するための図である。

【図６】

ＩＣカード５０内のメモリ空間にエリアやサービスを登録するための手順を示したフローチャートである。

【図７】

暗証コード・サービス・データ・ブロックのデータ構造を模式的に示した図である。

【図８】

ユーザから入力された暗証コードに従って、サービスの起動又はエリアへのアクセス権を制御するための処理手順を示したフローチャートである。

【図９】

暗証コードの入力失敗回数によりサービスやエリアへのアクセス権制御を行なうための処理手順を示したフローチャートである。

【図１０】

ＩＣカード５０における暗証コード比較出力の制御に関する機能構成を模式的に示した図である。

【図１１】

通信部１５１を介して１バイト単位で送受信されるデータの構造を模式的に示した図である。

【図１２】

１バイト・データが集まって構成されるパケットの構成を模式的に示した図である。

【図１３】

送受信者間におけるパケット交換の基本シーケンスを示した図である。

【図１４】

フロー制御部１５５の構成を示した図である。

【図１５】

暗証コード保持部及び暗証コード比較部を複数個装備した暗証コード識別装置（ＩＣカード５０）の構成例を示した図である。

【図１６】

データ保持部５２の個々のメモリ領域に対して暗証コードをそれぞれ設定できるようにした暗証コード識別装置（ＩＣカード５０）の構成例を示した図である。

【符号の説明】

５０…ＩＣチップ

５１…ＲＦ部

５２…メモリ

５３…照合部

５４…有線インターフェース

５５…制御部

１０１…リーダ／ライタ

１５１…通信部

１５２…データ保持部

１５３…暗証コード保持部

１５４…暗証コード比較部

１５５…フロー制御部

１５５Ａ…有効／無効フラグ

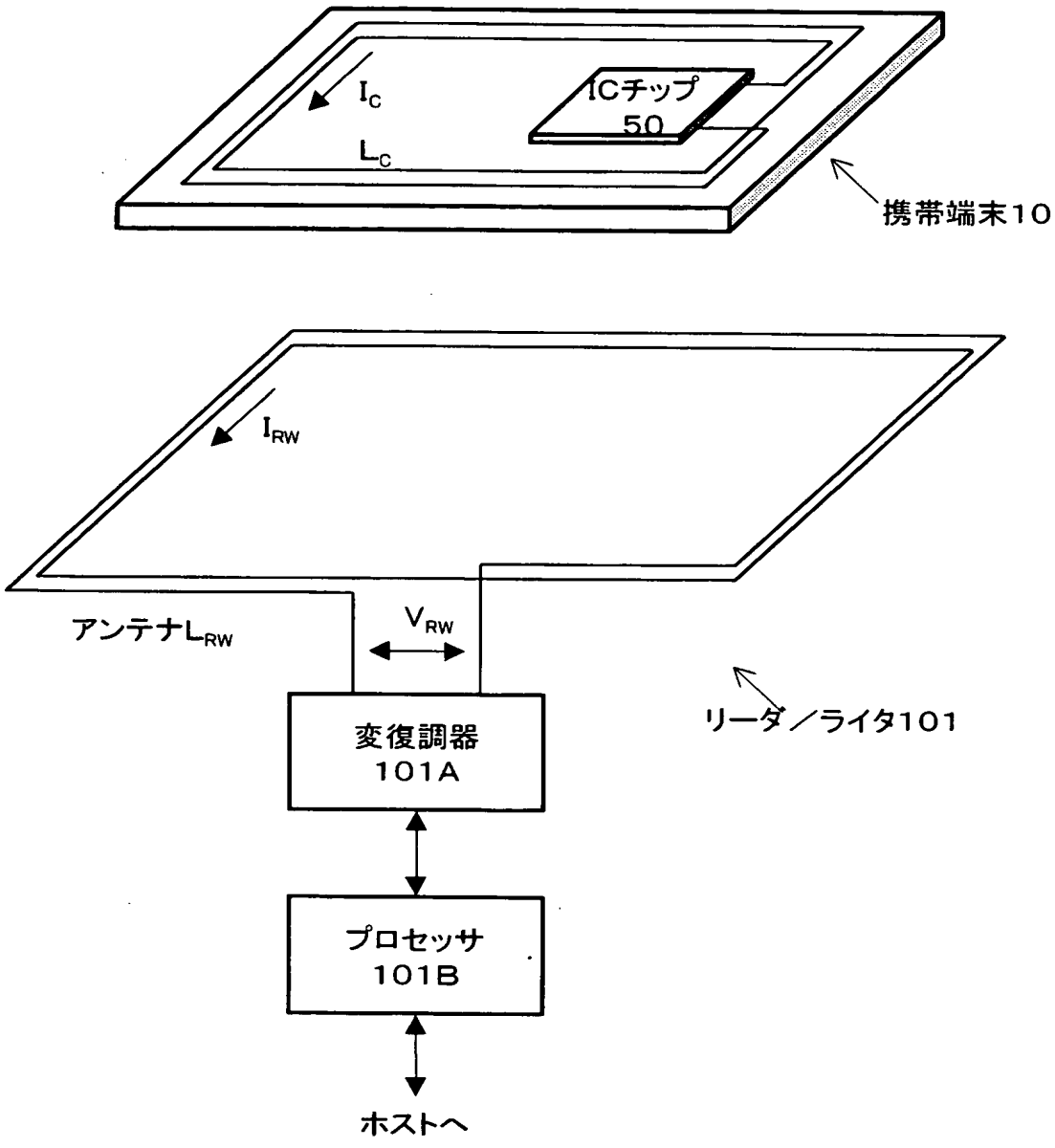
１５５Ｂ…無効→有効フラグ

１５５Ｃ…有効→無効フラグ

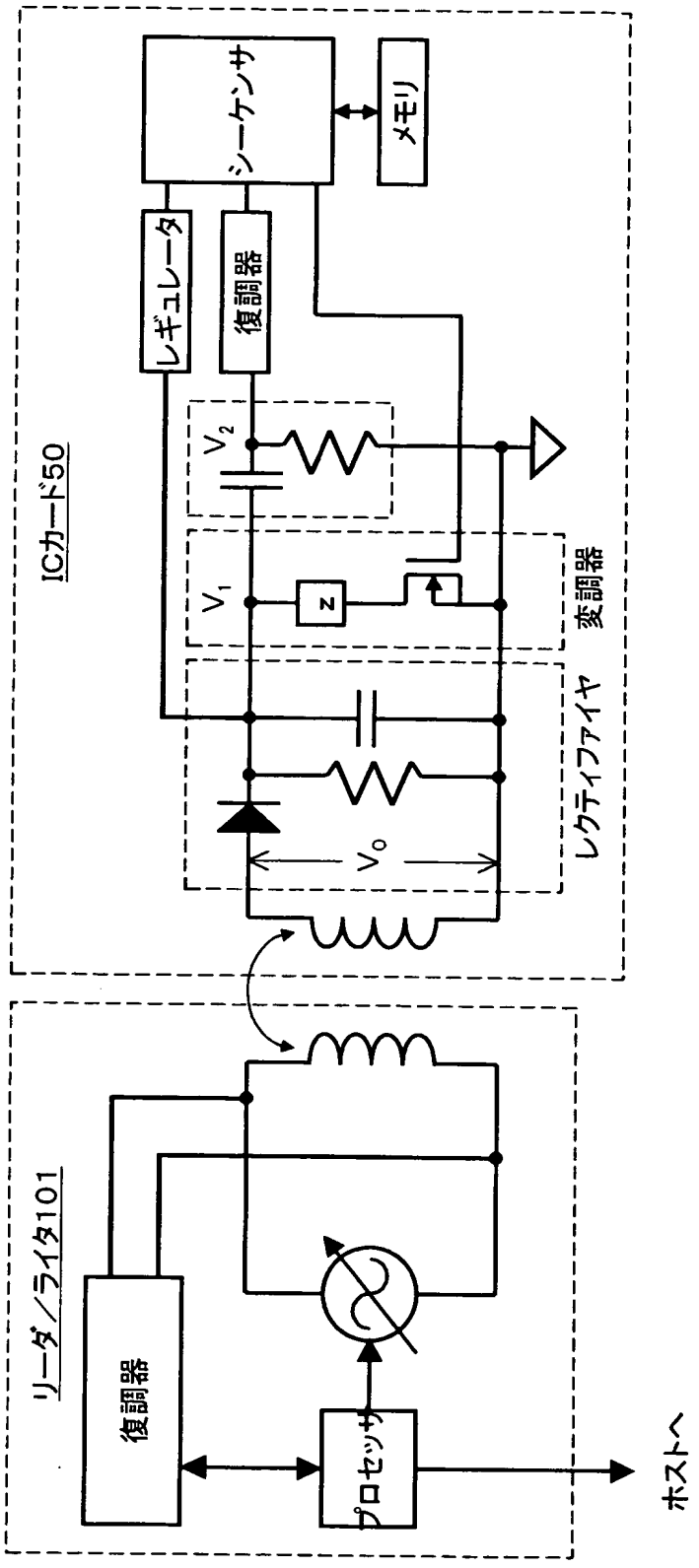
１５５Ｄ…フラグ判別部

【書類名】　図面

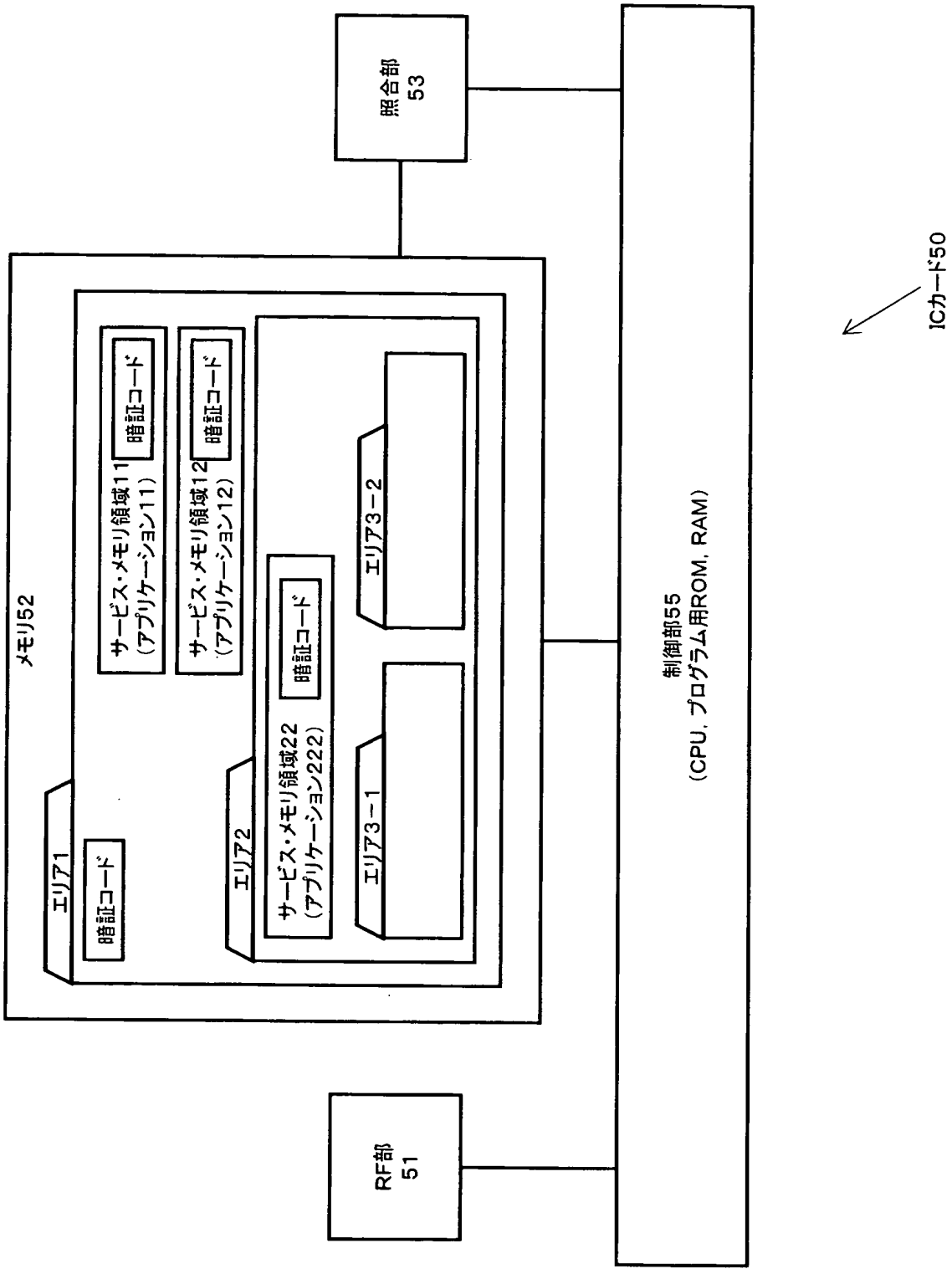
【図１】


I_C
L_C
ICチップ
50
携帯端末10
I_{RW}
アンテナL_{RW}
V_{RW}
リーダ／ライタ101
変復調器
101A
プロセッサ
101B
ホストへ

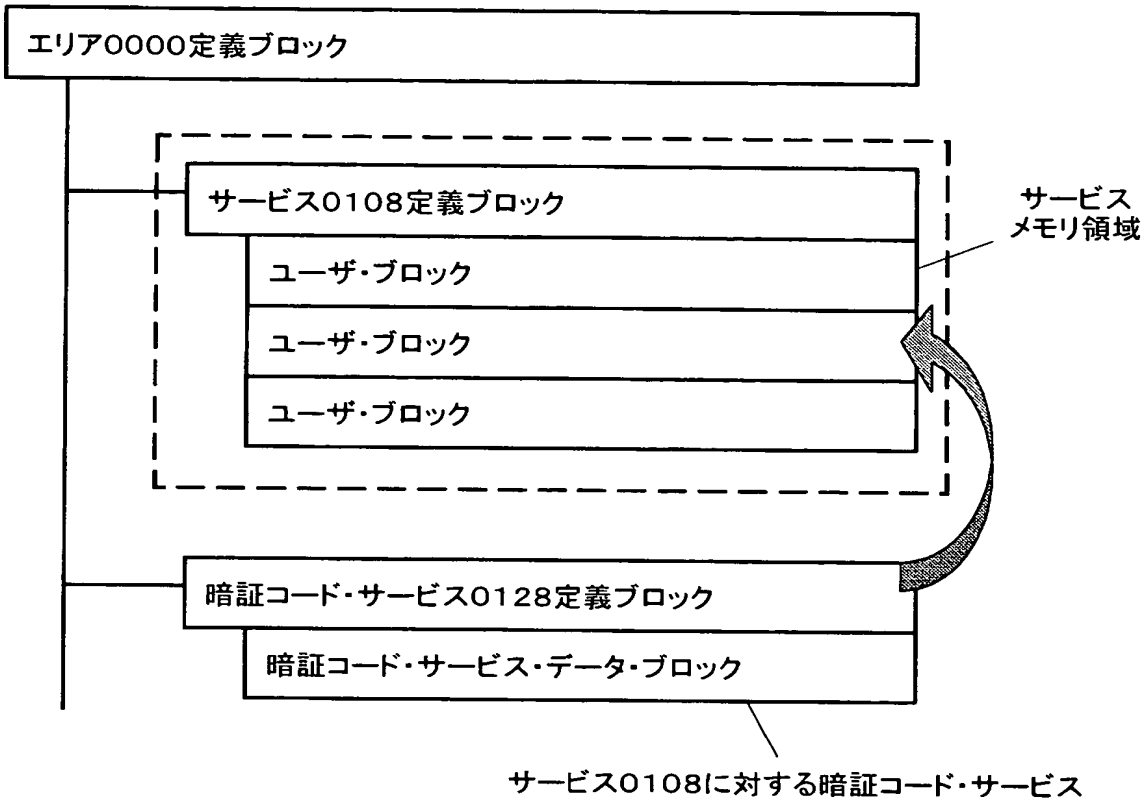
【図２】


ICカード50
シーケンサ
メモリ
レギュレータ
復調器
V_2
V_1
Z
変調器
レクティファイヤ
V_0
リーダ／ライタ101
復調器
プロセッサ
ホストへ

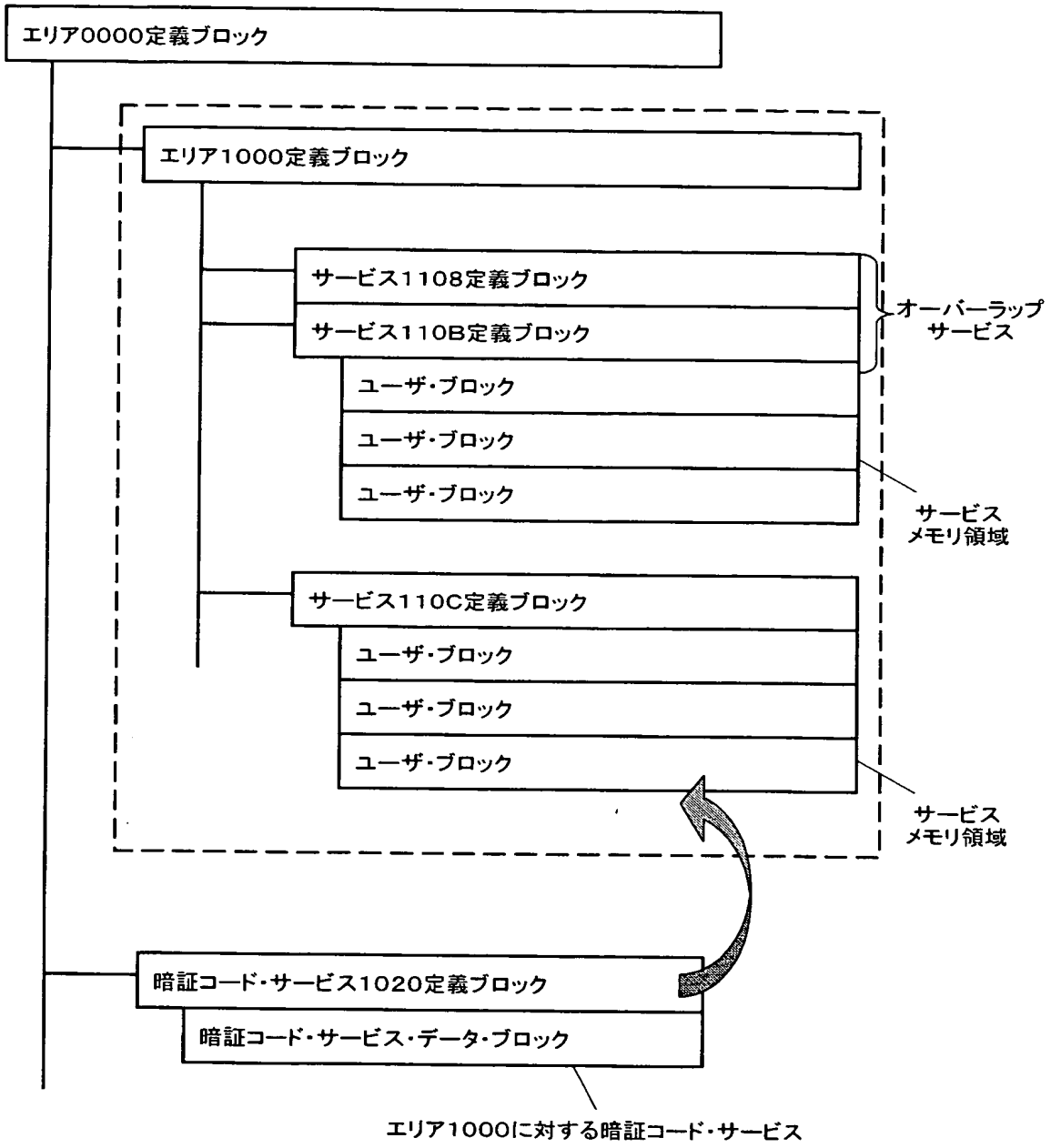
【図３】


照合部
53
ICカード50
メモリ52
エリア1
暗証コード
サービス・メモリ領域11
(アプリケーション11)
暗証コード
サービス・メモリ領域12
(アプリケーション12)
暗証コード
エリア2
サービス・メモリ領域22
(アプリケーション222)
暗証コード
エリア3－1
エリア3－2
制御部55
(CPU, プログラム用ROM, RAM)
RF部
51

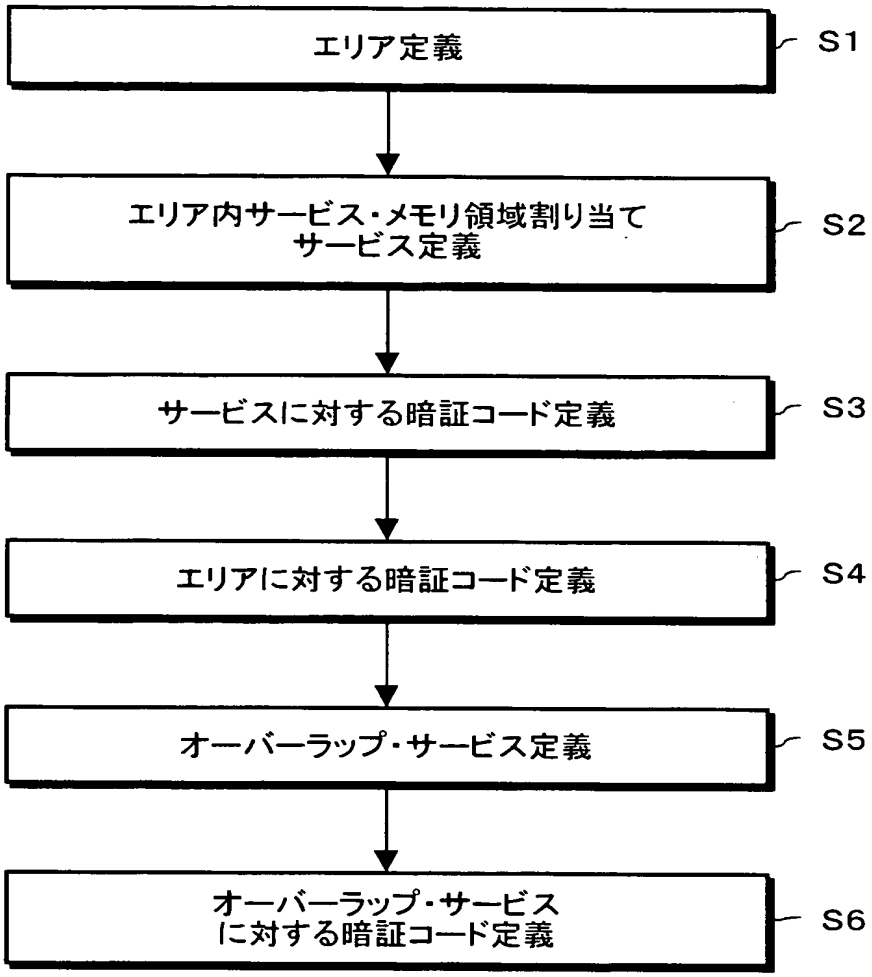
【図４】


エリア0000定義ブロック
サービス0108定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス0128定義ブロック
暗証コード・サービス・データ・ブロック
サービス0108に対する暗証コード・サービス

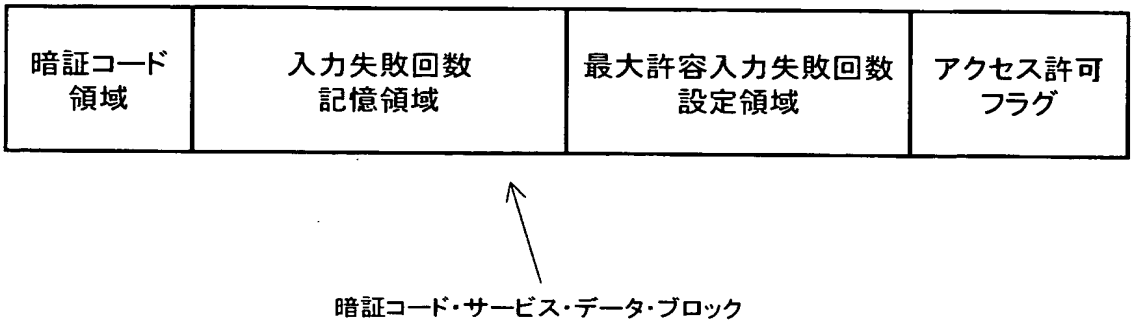
【図５】


エリア0000定義ブロック
エリア1000定義ブロック
サービス1108定義ブロック
サービス110B定義ブロック
オーバーラップ
サービス
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
サービス110C定義ブロック
ユーザ・ブロック
ユーザ・ブロック
ユーザ・ブロック
サービス
メモリ領域
暗証コード・サービス1020定義ブロック
暗証コード・サービス・データ・ブロック
エリア1000に対する暗証コード・サービス

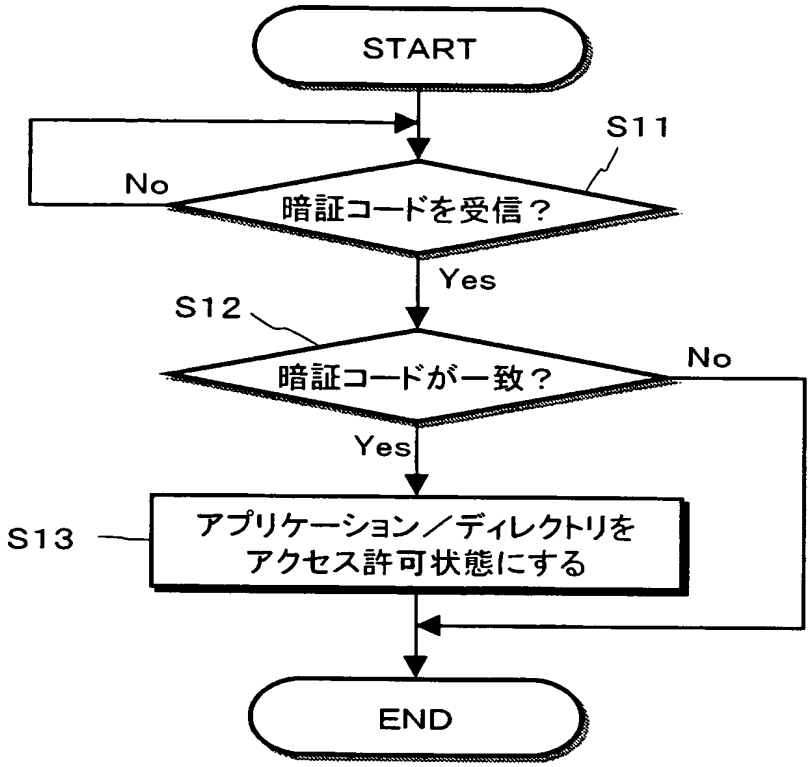
【図６】


エリア定義
S1
エリア内サービス・メモリ領域割り当て
サービス定義
S2
サービスに対する暗証コード定義
S3
エリアに対する暗証コード定義
S4
オーバーラップ・サービス定義
S5
オーバーラップ・サービス
に対する暗証コード定義
S6

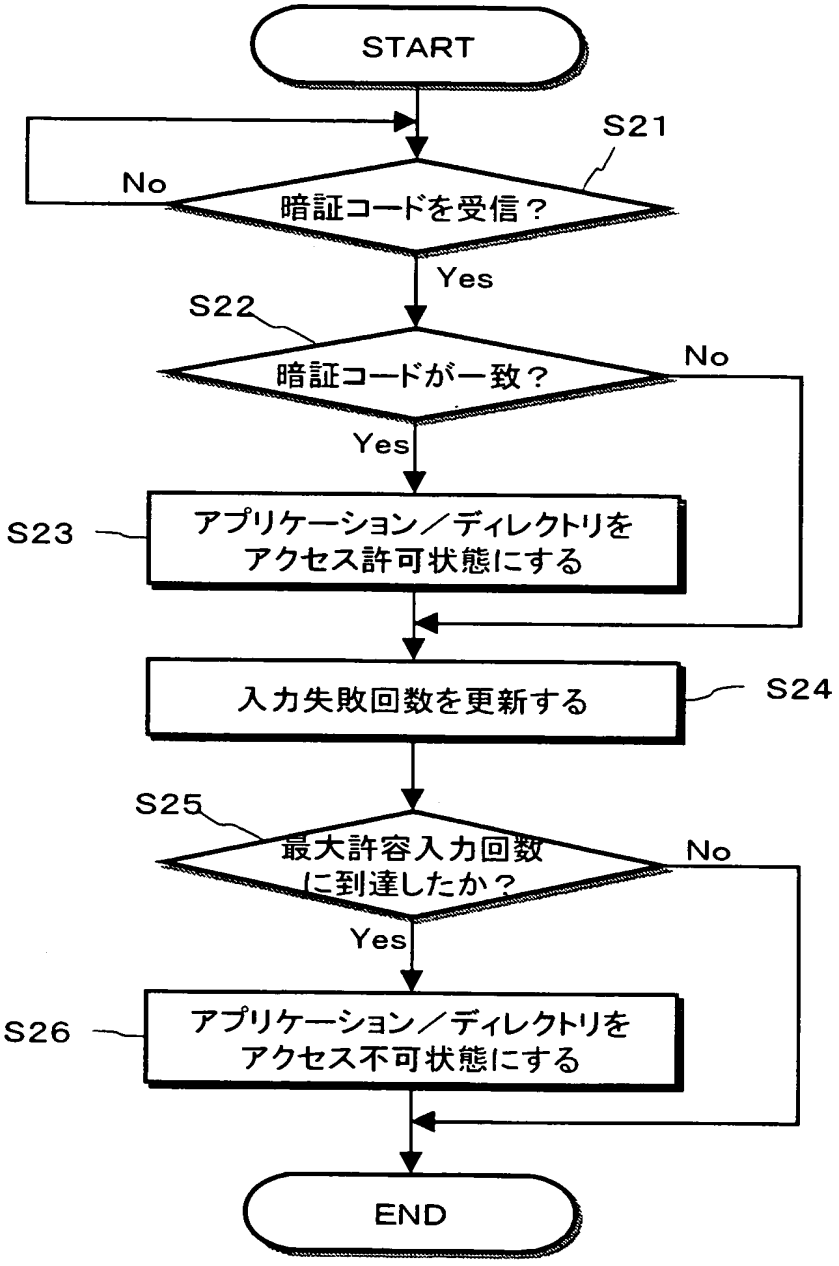
【図７】


暗証コード
領域
入力失敗回数
記憶領域
最大許容入力失敗回数
設定領域
アクセス許可
フラグ
暗証コード・サービス・データ・ブロック

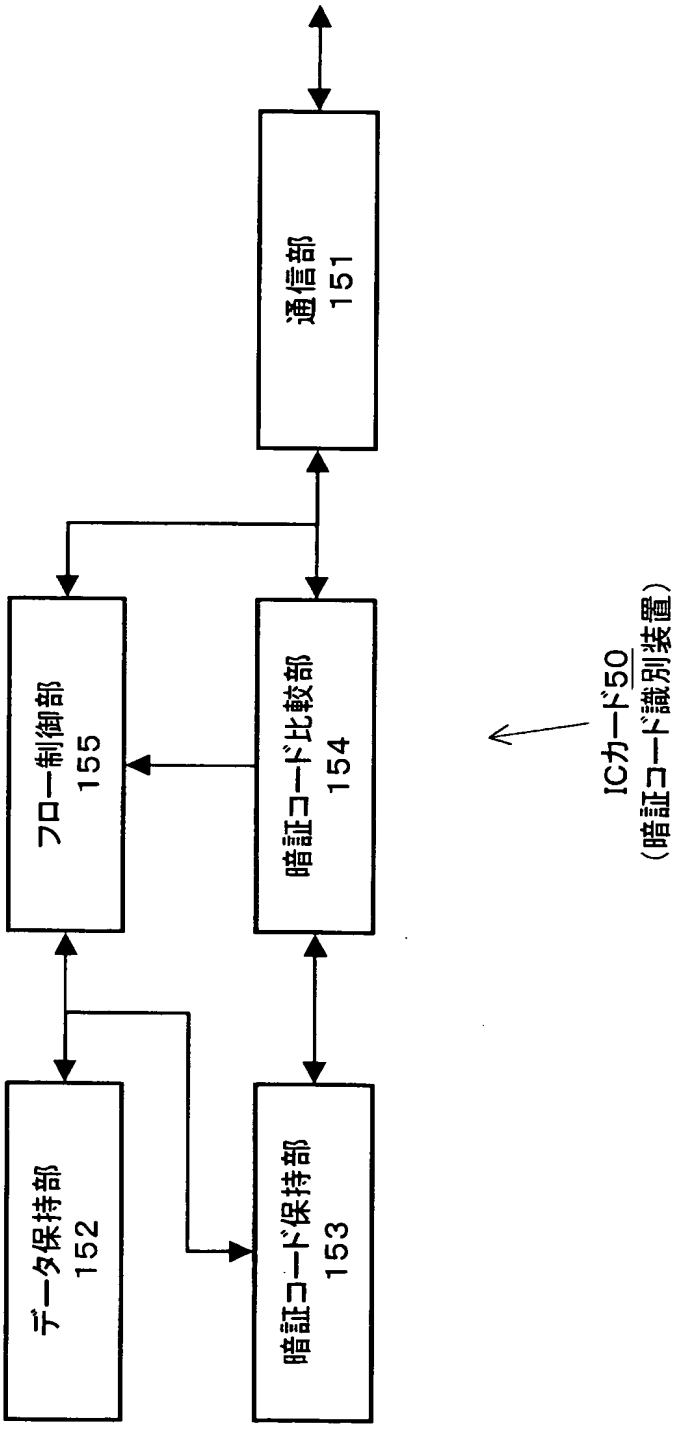
【図８】


START
S11
No
暗証コードを受信？
Yes
S12
暗証コードが一致？
No
Yes
S13
アプリケーション／ディレクトリを
アクセス許可状態にする
END

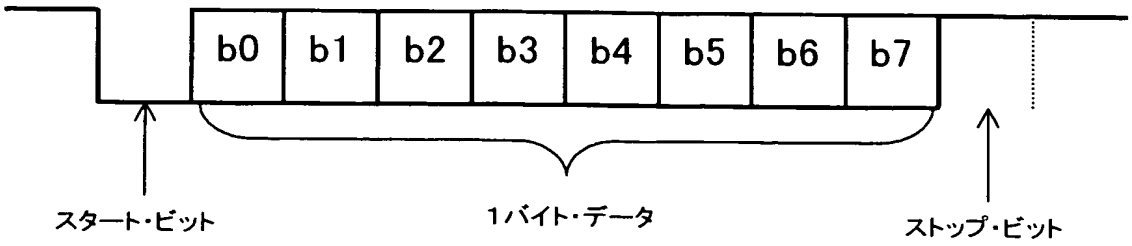
【図９】


START
S21
No
暗証コードを受信？
Yes
S22
暗証コードが一致？
No
Yes
S23
アプリケーション／ディレクトリを
アクセス許可状態にする
入力失敗回数を更新する
S24
S25
最大許容入力回数
に到達したか？
No
Yes
S26
アプリケーション／ディレクトリを
アクセス不可状態にする
END

【図１０】

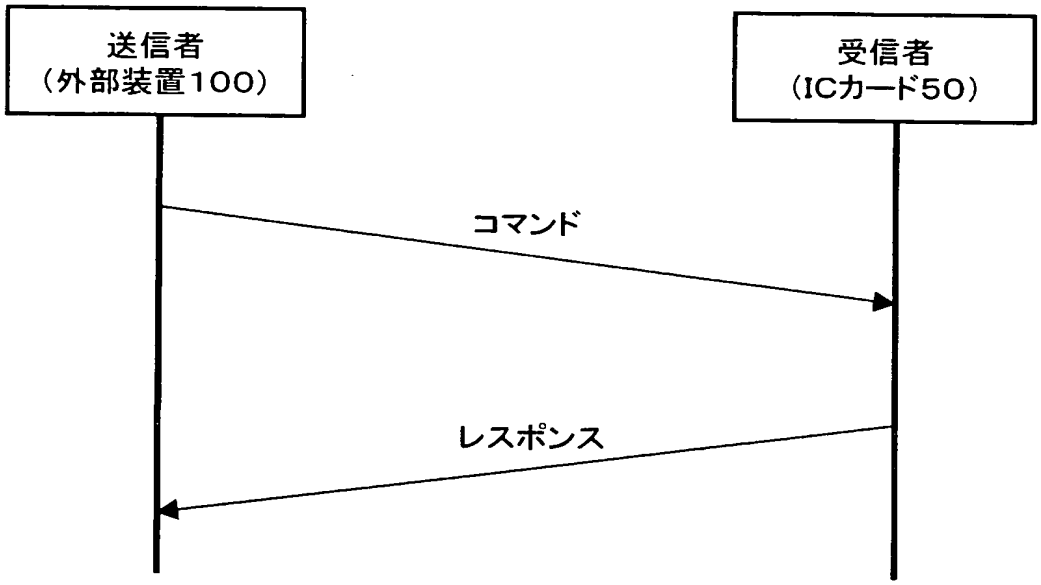

通信部
151
フロー制御部
155
暗証コード比較部
154
ICカード50
(暗証コード識別装置)
データ保持部
152
暗証コード保持部
153

【図１１】

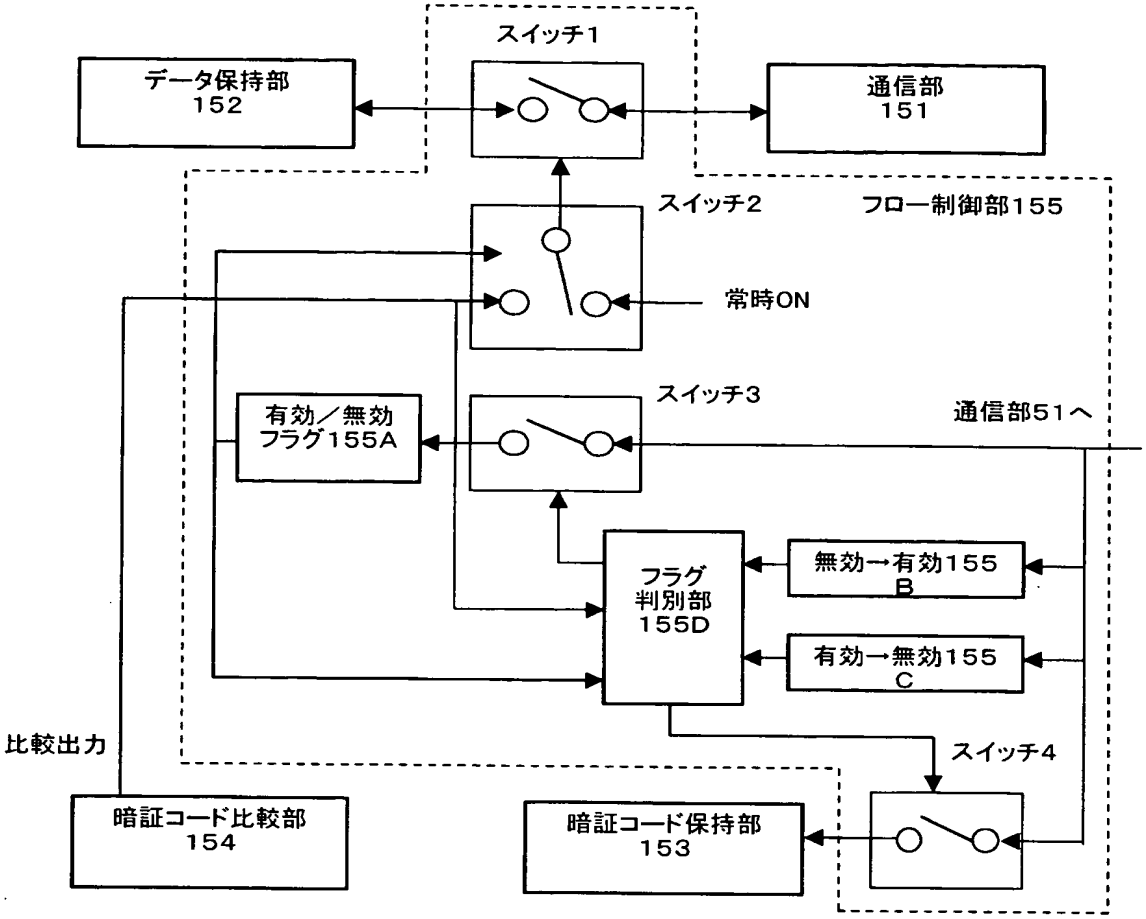


【図１２】

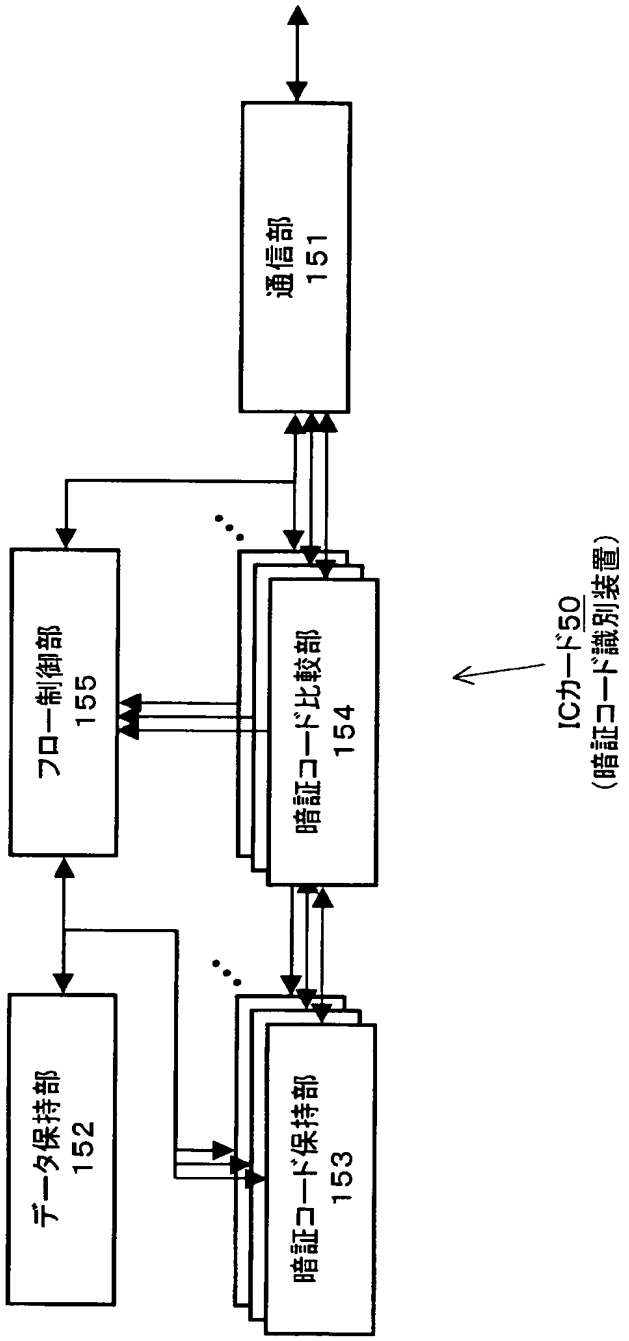
【図１３】



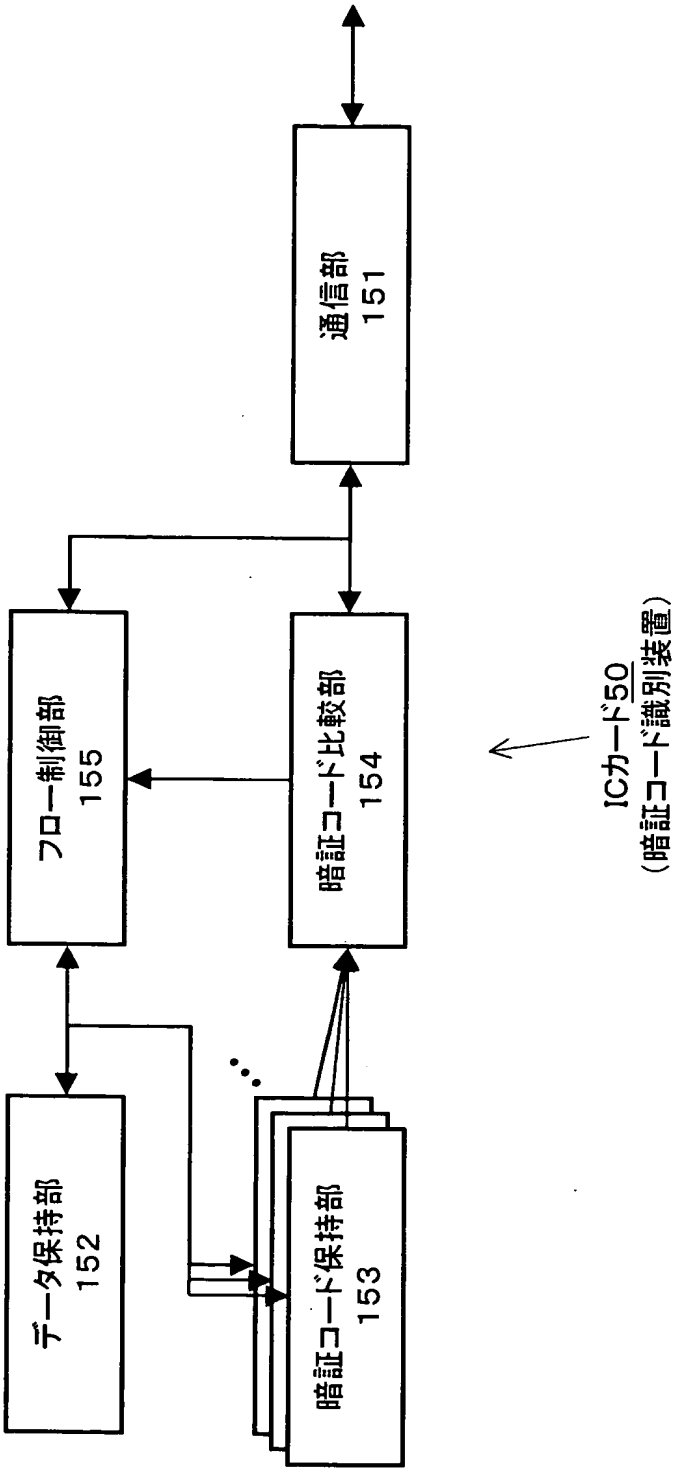
【図１４】


スイッチ1
データ保持部
152
通信部
151
スイッチ2
フロー制御部155
常時ON
スイッチ3
有効／無効
フラグ155A
通信部51へ
フラグ
判別部
155D
無効→有効155
B
有効→無効155
C
スイッチ4
比較出力
暗証コード比較部
154
暗証コード保持部
153

【図１５】


通信部
151
フロー制御部
155
暗証コード比較部
154
データ保持部
152
暗証コード保持部
153
ICカード50
(暗証コード識別装置)

【図１６】


通信部
151
フロー制御部
155
暗証コード比較部
154
ICカード50
（暗証コード識別装置）
データ保持部
152
暗証コード保持部
153

【書類名】　要約書

【要約】

【課題】　サービス・メモリ領域に対して複数のアクセス方法と、アクセス方法毎のアクセス権限を提供する。

【解決手段】　１つのサービス・メモリ領域に対して、複数サービスを重複して定義し（オーバーラップ・サービス）、サービス・メモリ領域に「読み出しのみ」、「読み出し及び書き込み」など複数のアクセス方法を設定する。オーバーラップ・サービス定義を行なう場合、サービス毎に暗証コードを設定するようにしてもよい。例えば、同じサービス・メモリ領域に対して起動するサービスが「読み出し」と「読み出し及び書き込み」とでは、別々の暗証コードが設定される。

【選択図】　図５

特願２００３－１０４７０６

出　願　人　履　歴　情　報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社